Some Thoughts about Applying STAMP to Environmental-Sociotechnical Systems (ESTS) – Very Complex System of Systems (SoS)

Second STAMP Conference

2013

Daniel Hartmann, PhD

Management & Safety Engineering Unit, Ben-Gurion University

Beer Sheva, Israel

A wider look at STAMP (System-Theoretic Accident Model and Processes)

- **Data – Information – Knowledge – Context [D.I.K.C.]**

- ✓ **System Theory**
- ✓ **Hierarchical Safety Control Structure**
- ✓ **Process Models**
- ✓ **Safety Constraints**

Data – Information – Knowledge – Context [D.I.K.C.]

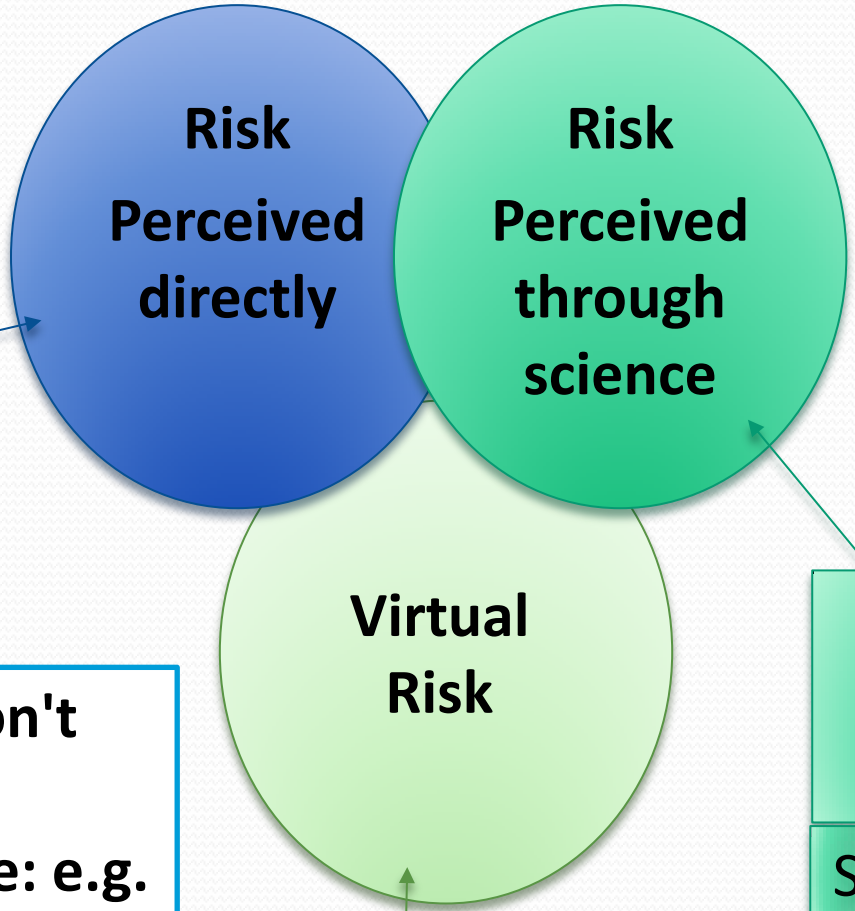
- **Data** is the lowest level of abstraction, collected by "sensors" and leading to **describing** “something” or a process.
- **Information** is a medium level of abstraction, processed by "brain" and an exciting "model" and leading to **understanding** of "something" or a process.
- **Knowledge** is the highest level of abstraction, processed by "brain" and an exciting "model" and leading to **action** related to "something" or a process.

However, Risk is dictated by D.I.K.C.

e.g. using fire, cutting with a knife, climbing a tree

Natural DIKC

System 1 thinking



e.g. cholera need a microscope to see it and a scientific training to understand it

Scientific DIKC = Complexity

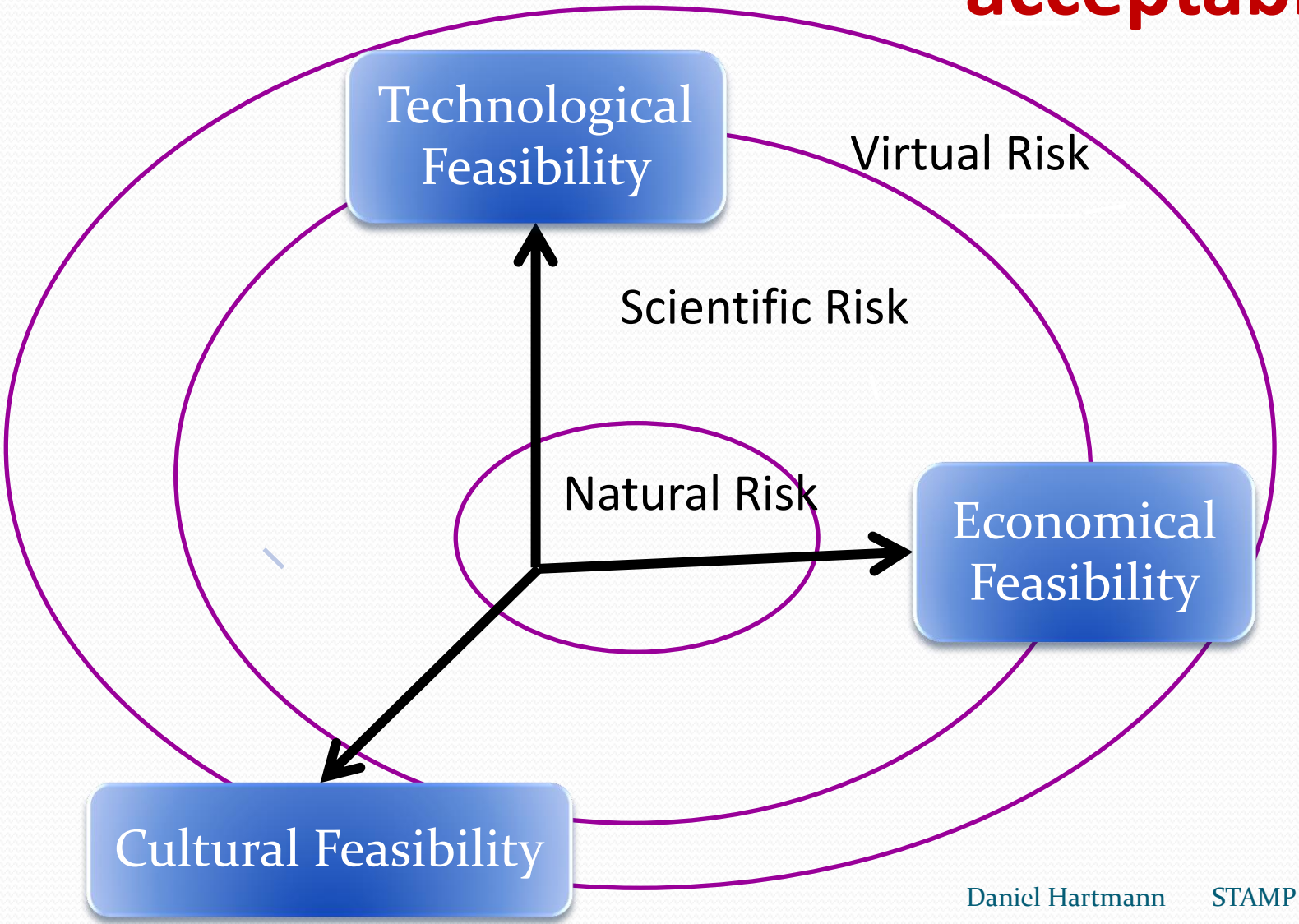
System 2 thinking

Scientists don't know yet or cannot agree: e.g. global warming, mobile phones

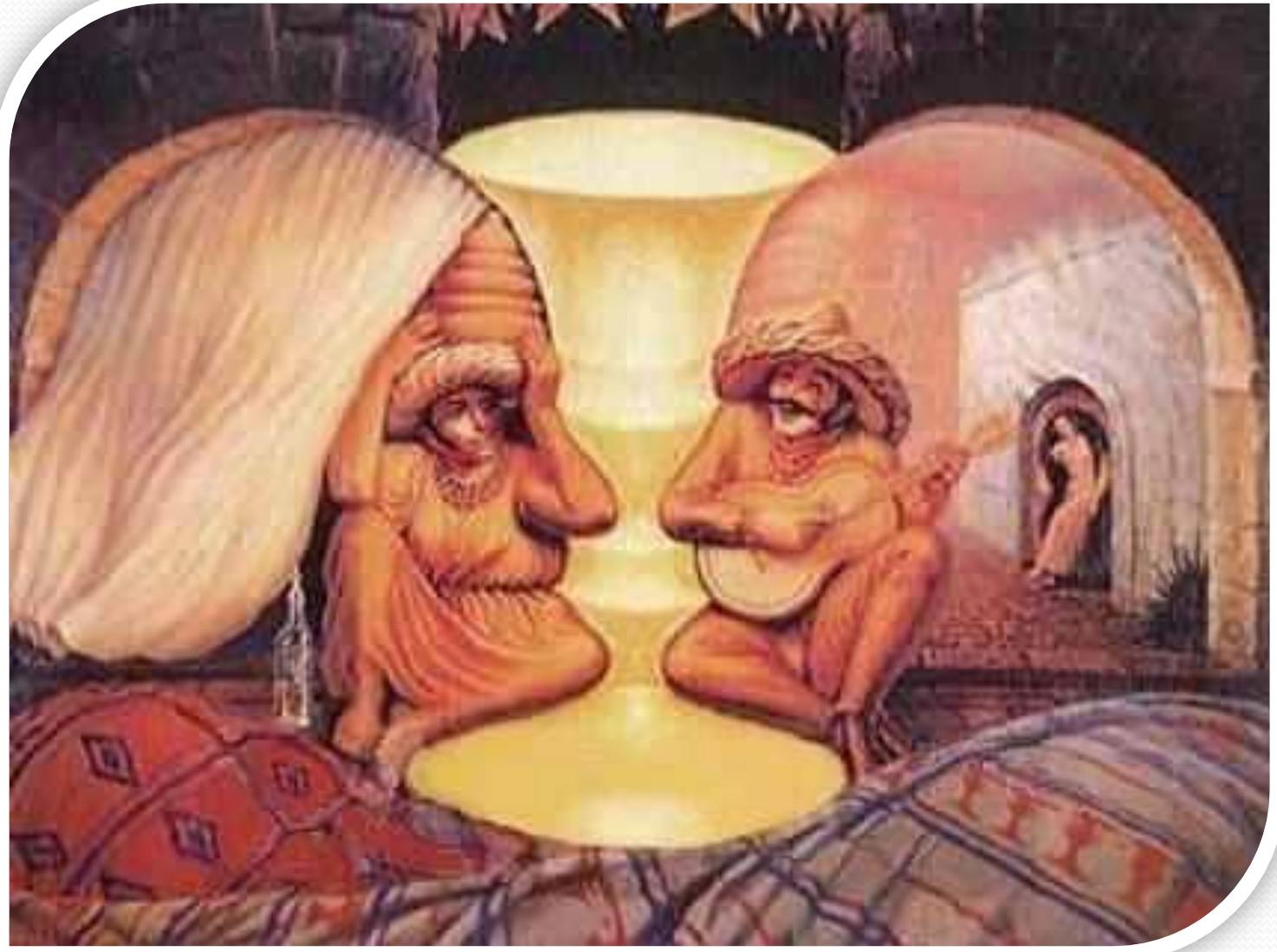
Virtual DIKC

After Adams (1999)

More Fundamentals dictating level of acceptable Risk



One Picture - Two Perceptions



D.I.K.C., *Perception* and Process Models?

Perception is the process of attaining awareness or understanding of the situation by organizing and interpreting sensory information.

Whos Perception? Who Creates it? Who Controls it? Etc...

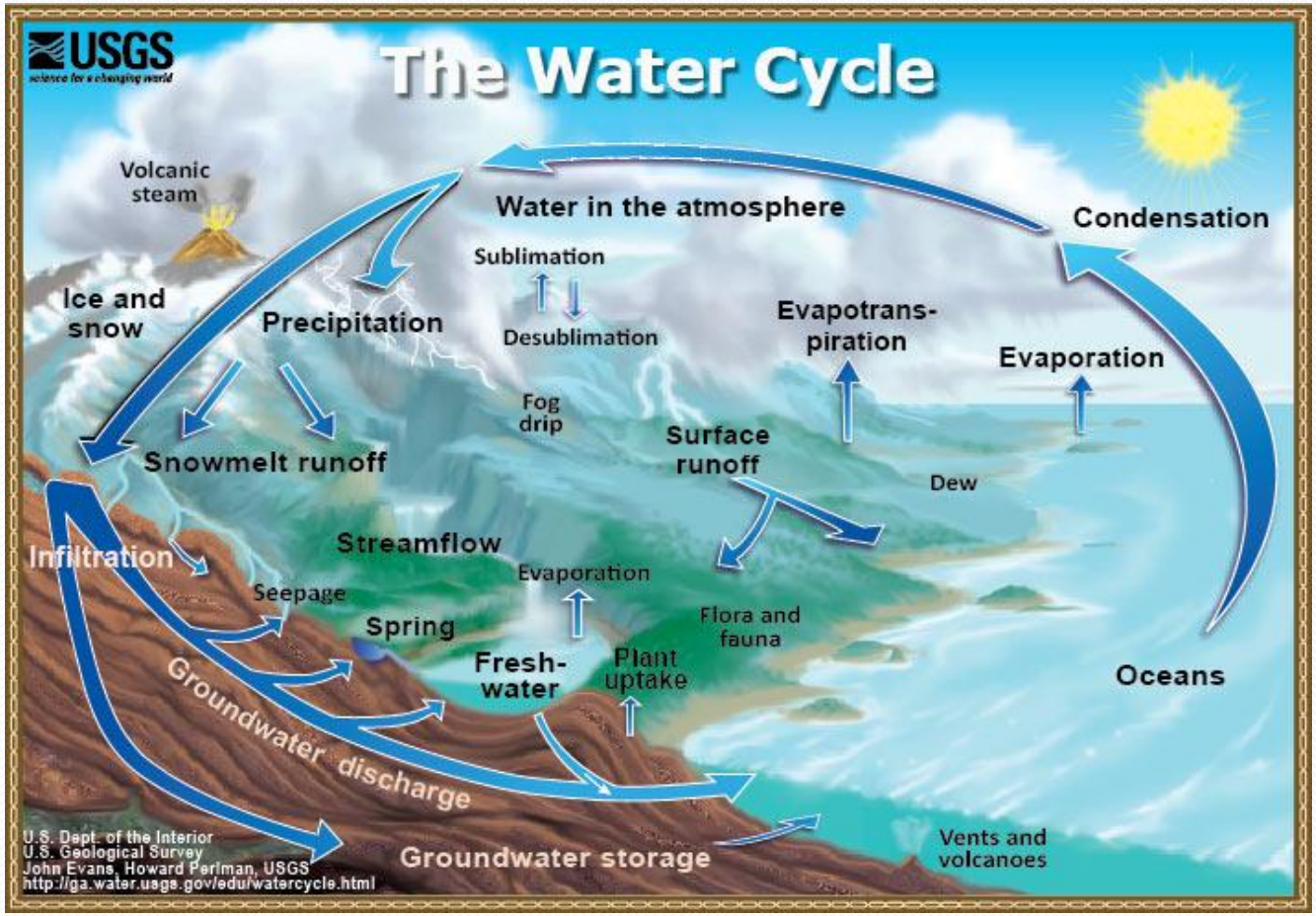
- "End User"?
- "Scientists"?
- Low Level Controller?
- Medium Level Controller?
- High Level Sociotechnical Controller?
- High Level Environmental Controller?

A wider look at STAMP

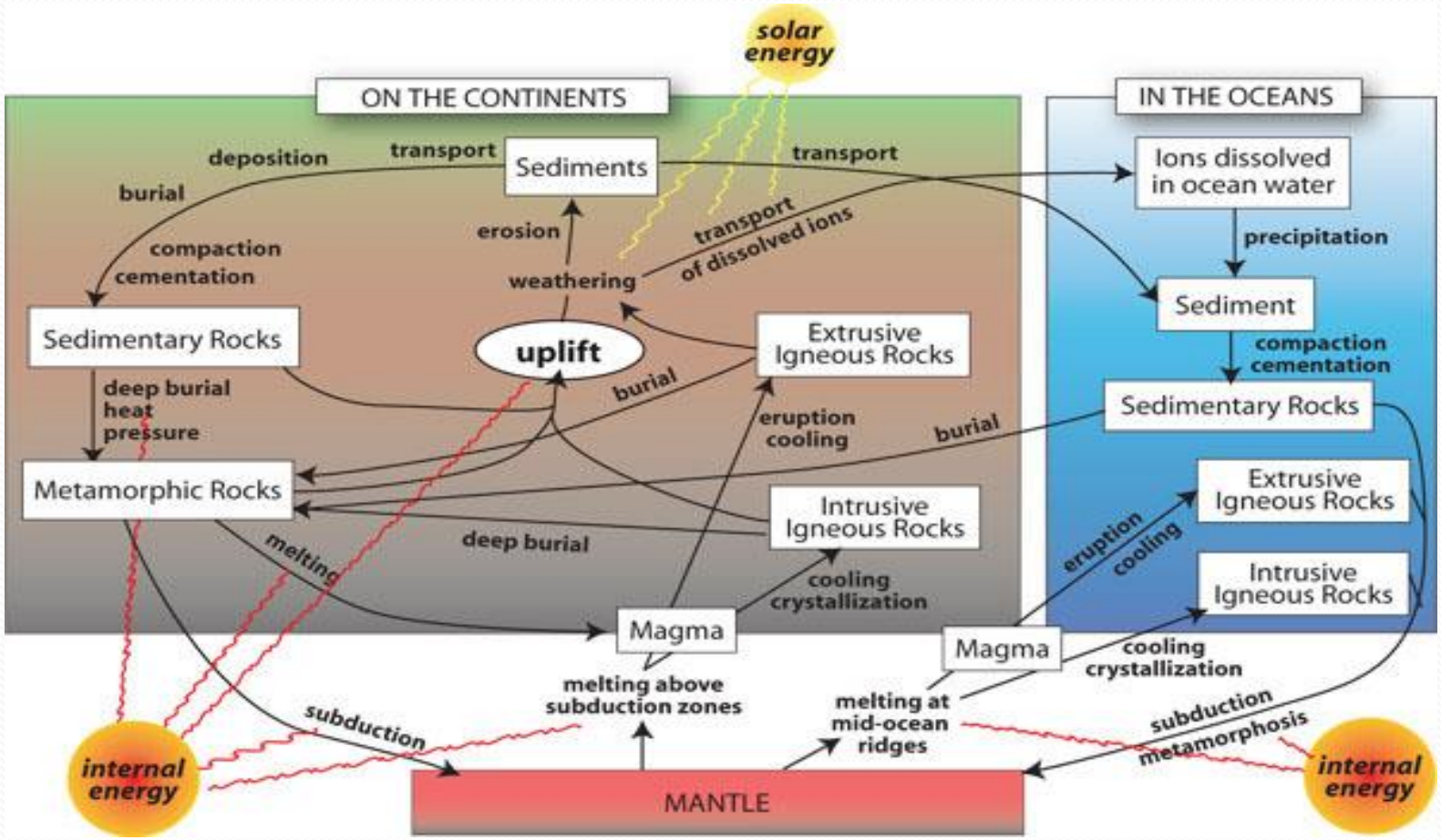
(System-Theoretic Accident Model and Processes)

- ➢ **Data – Information – Knowledge – Context [D.I.K.C.]**
- ✓ **System Theory**
- ✓ **Hierarchical Safety Control Structure**
- ✓ **Process Models**
- ✓ **Safety Constraints**

Environmental System of Systems

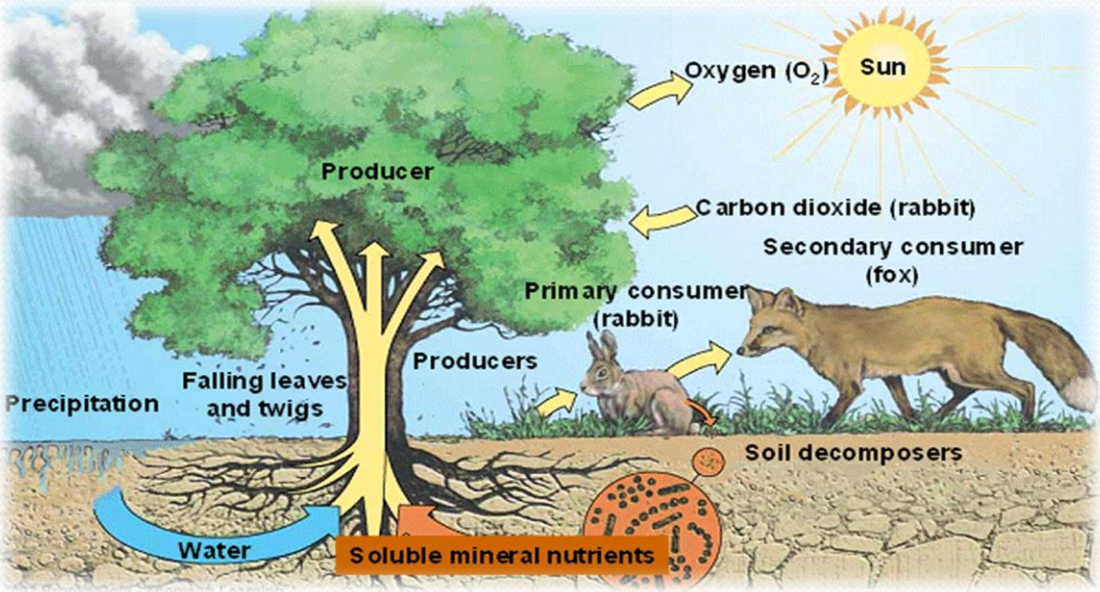


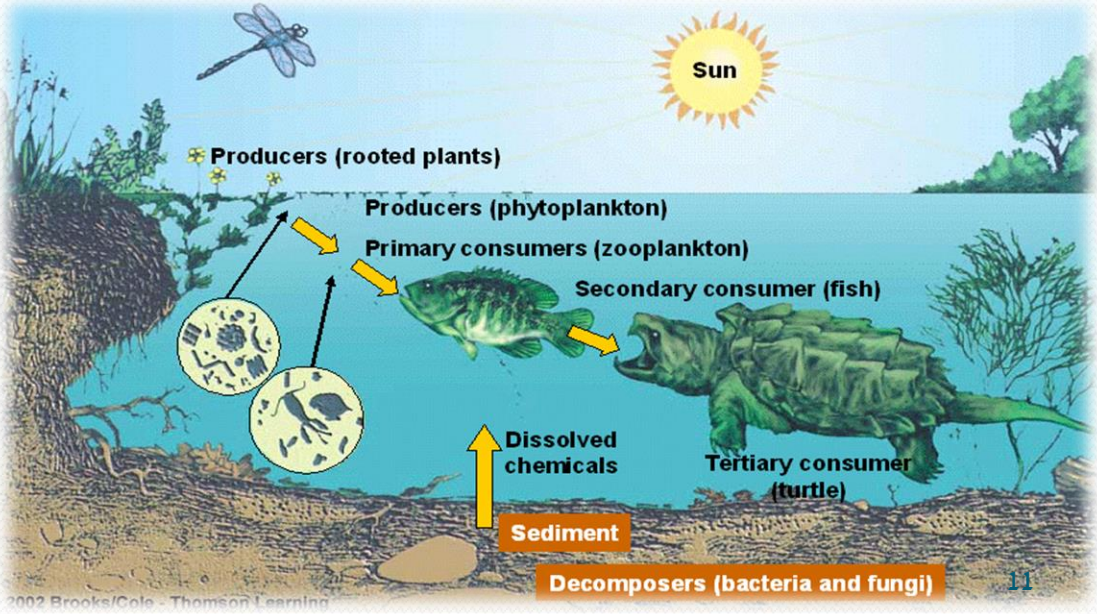
Environmental System of Systems
The Rock Cycle



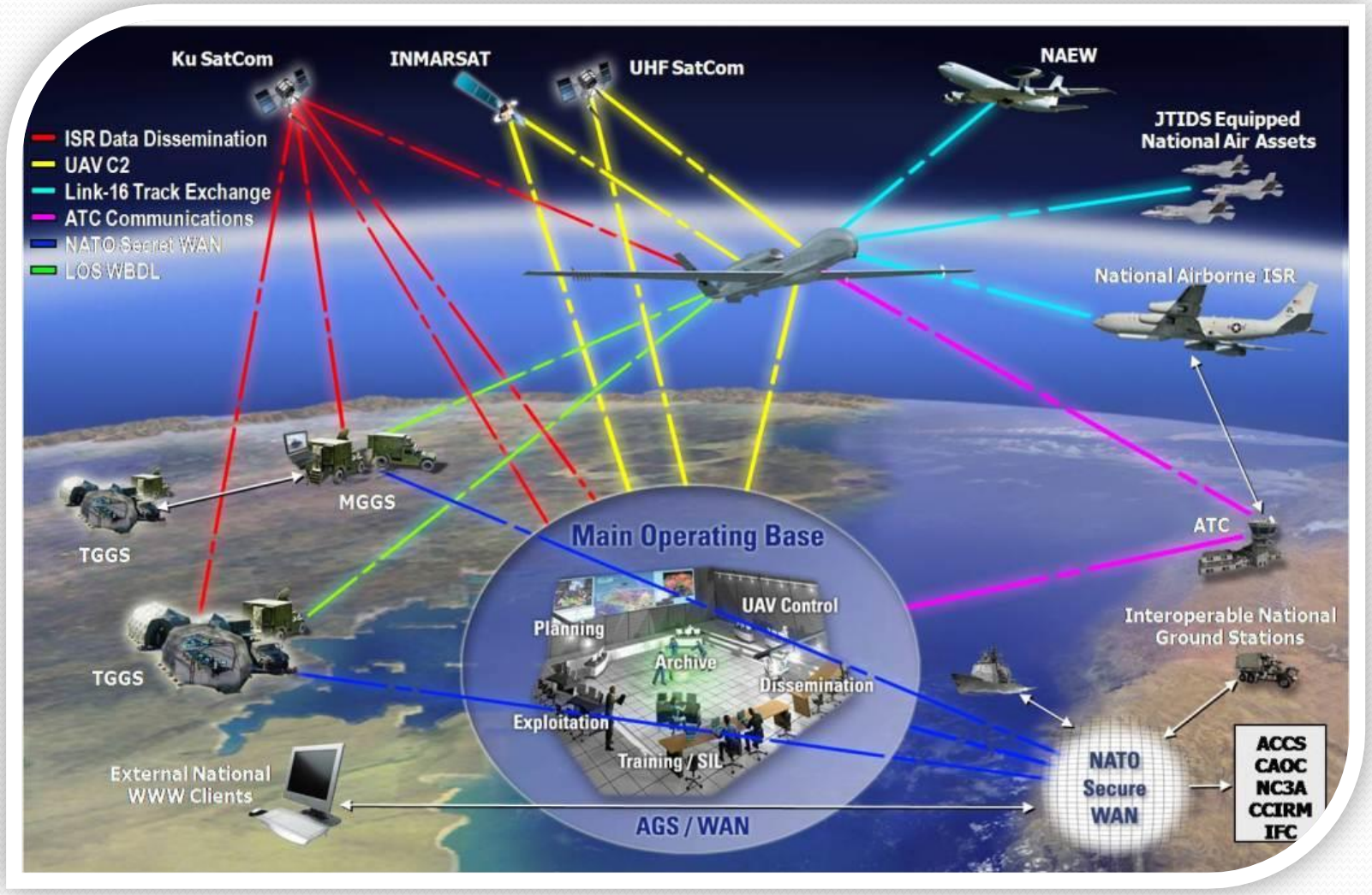
Environmental System of Systems

Eco-Systems





Modern Battlefield and the Environment

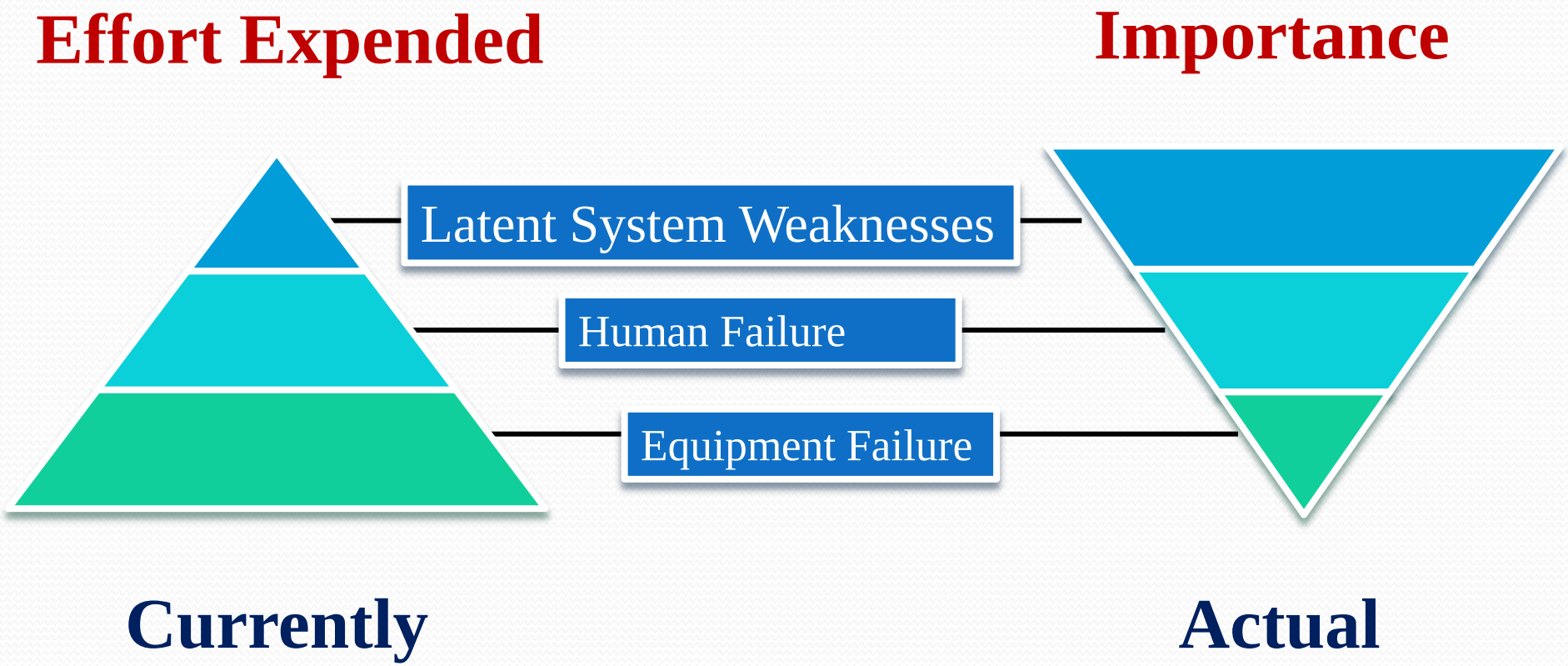


Some “New” Ideas about System Boundaries

Egocentric → System-centric

Sociotechnical → Environmental-Sociotechnical

Effort vs. Importance*



* Adapted from Kletz, T. (2001), *An Engineer's View of Human Error* (3rd ed.); p.127.

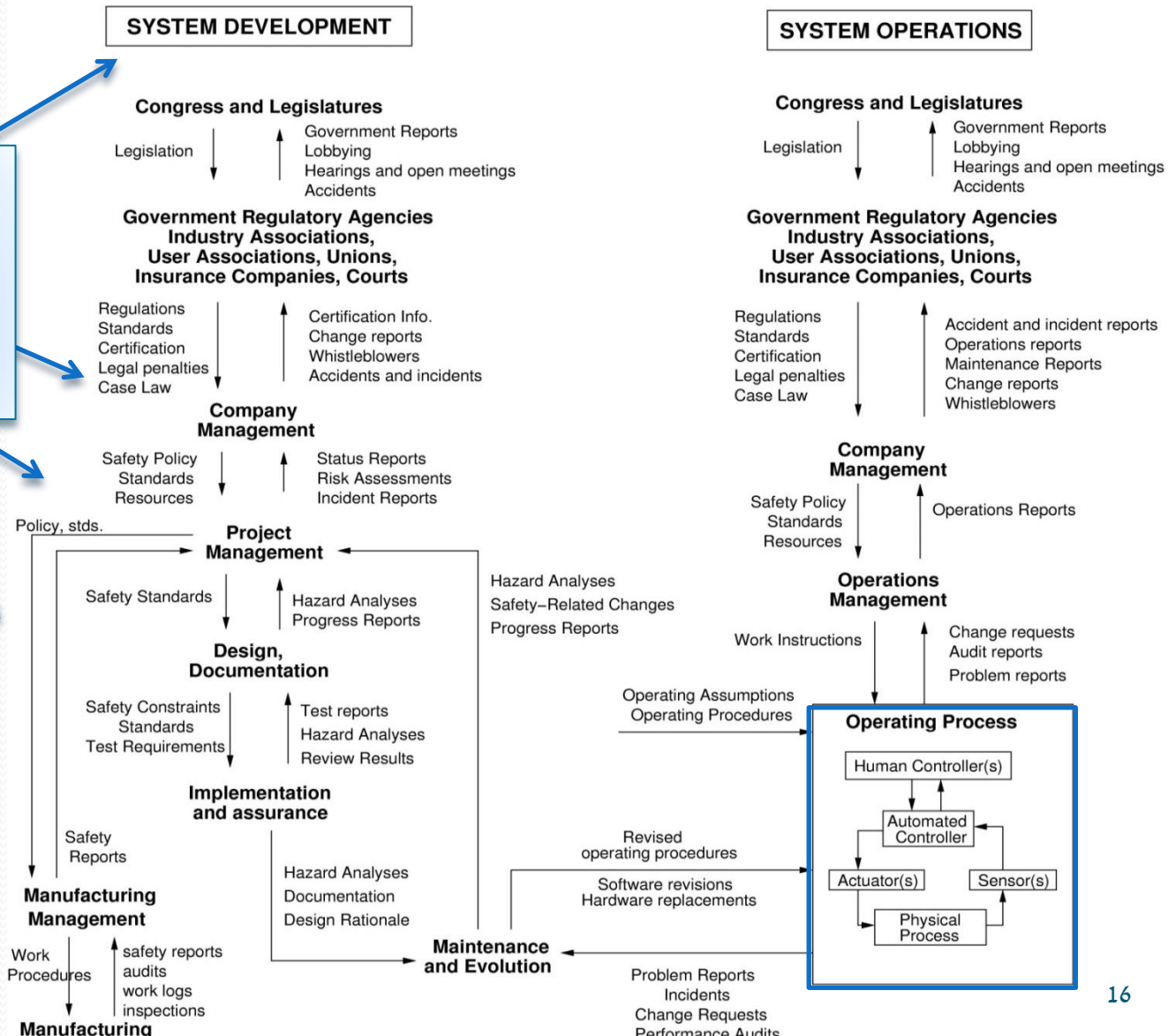
A wider look at STAMP

(System-Theoretic Accident Model and Processes)

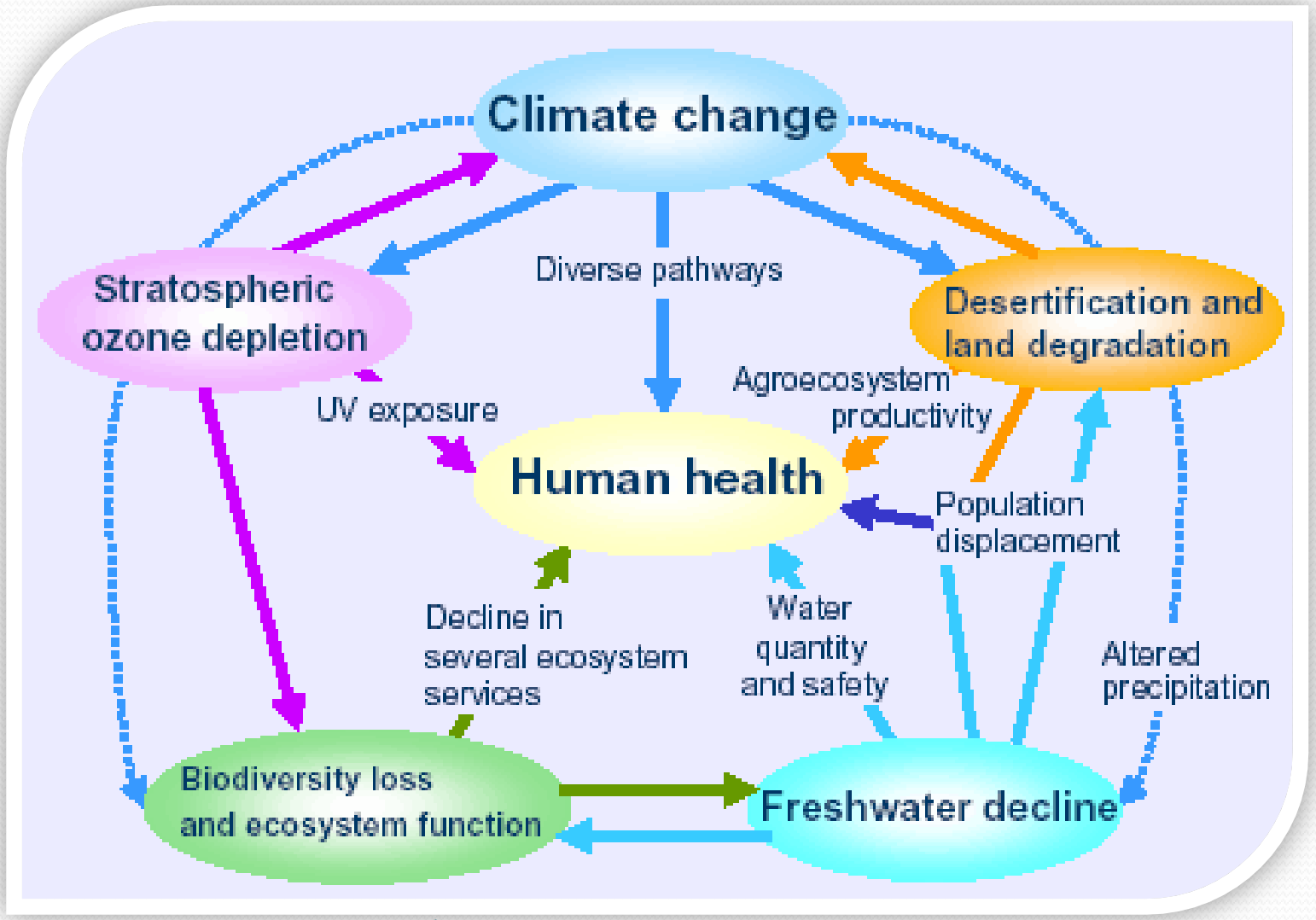
- ➢ **Data – Information – Knowledge – "Context" [D.I.K.C.]**
- ✓ **System Theory**
- ✓ **Hierarchical Safety Control Structure**
- ✓ **Process Models**
- ✓ **Safety Constraints**

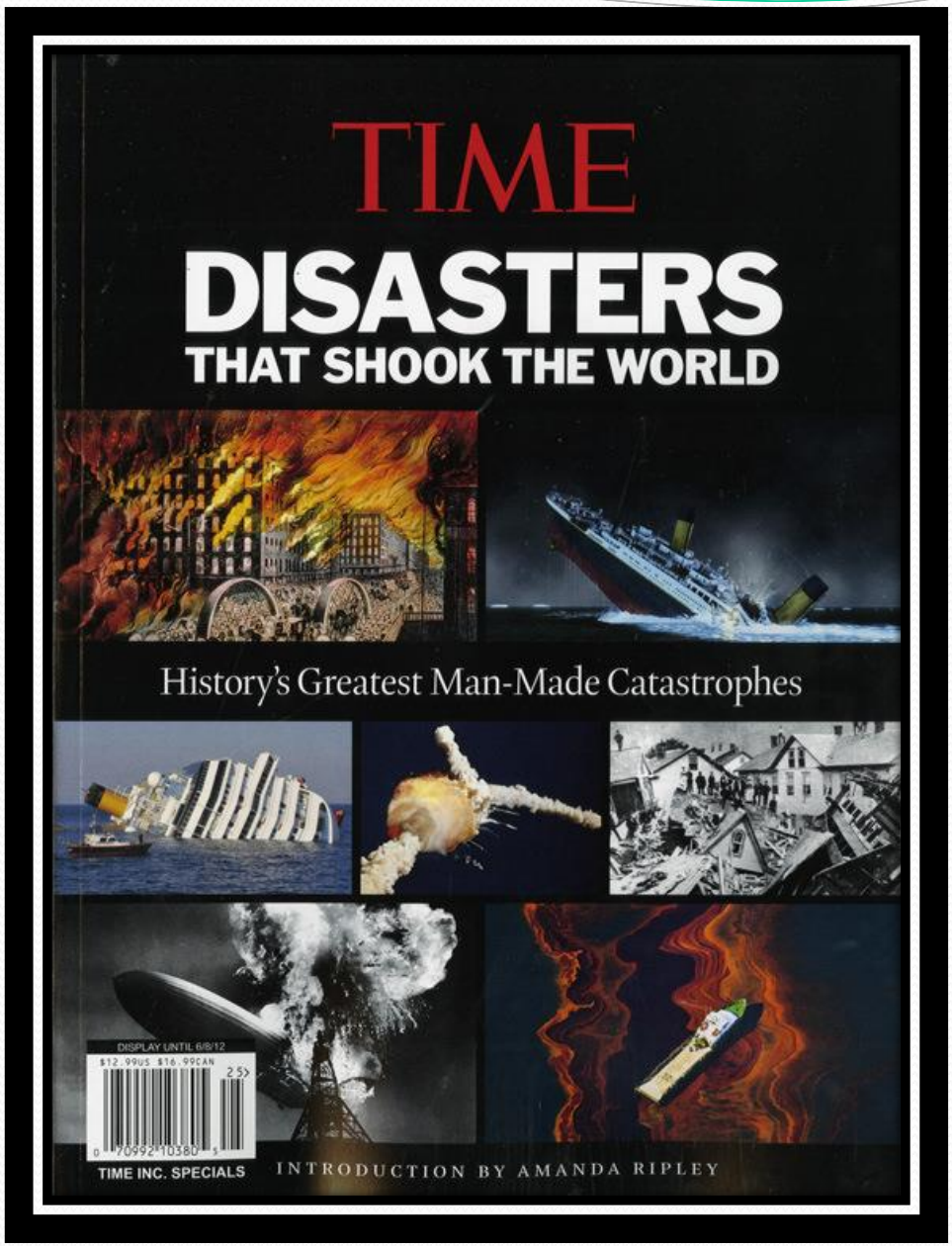
Example Safety Control Structure

Where starts System safety Engineering?



Environmental-Sociotechnical System




TIME
DISASTERS
THAT SHOOK THE WORLD
History's Greatest Man-Made Catastrophes
DISPLAY UNTIL 6/8/12
$12.99US $16.99CAN
TIME INC. SPECIALS
INTRODUCTION BY AMANDA RIPLEY

Force Majeure - Superior Force - Act of God - Chance Occurrence - Unavoidable Accident

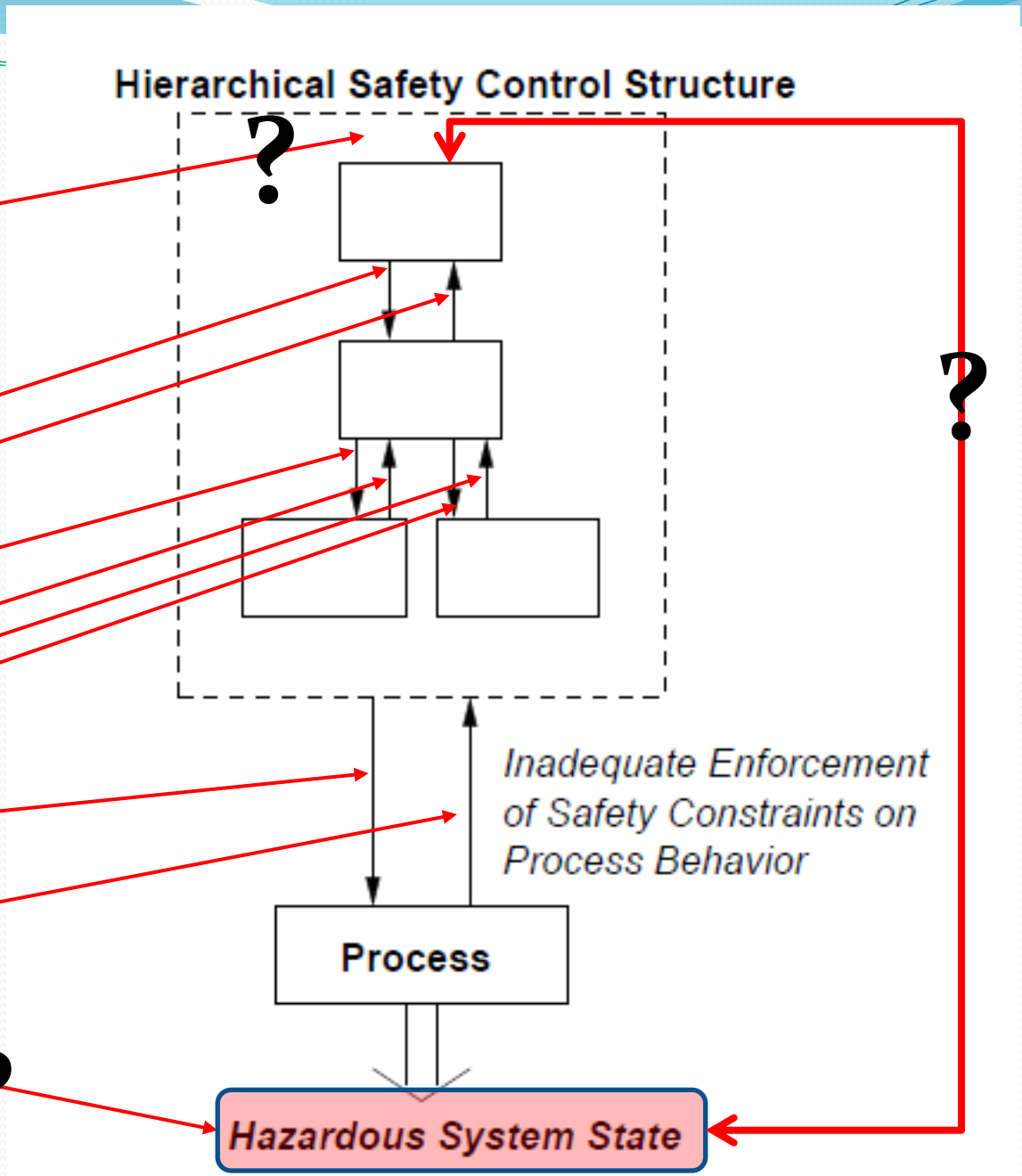
Resulting from:

- hurricane
- flooding
- earthquake
- volcanic eruption
- Virus pandemic
- Fire
- Dust storm
- Any unexpected / extreme environmental conditions
- etc.

Accident Causality Using STAMP

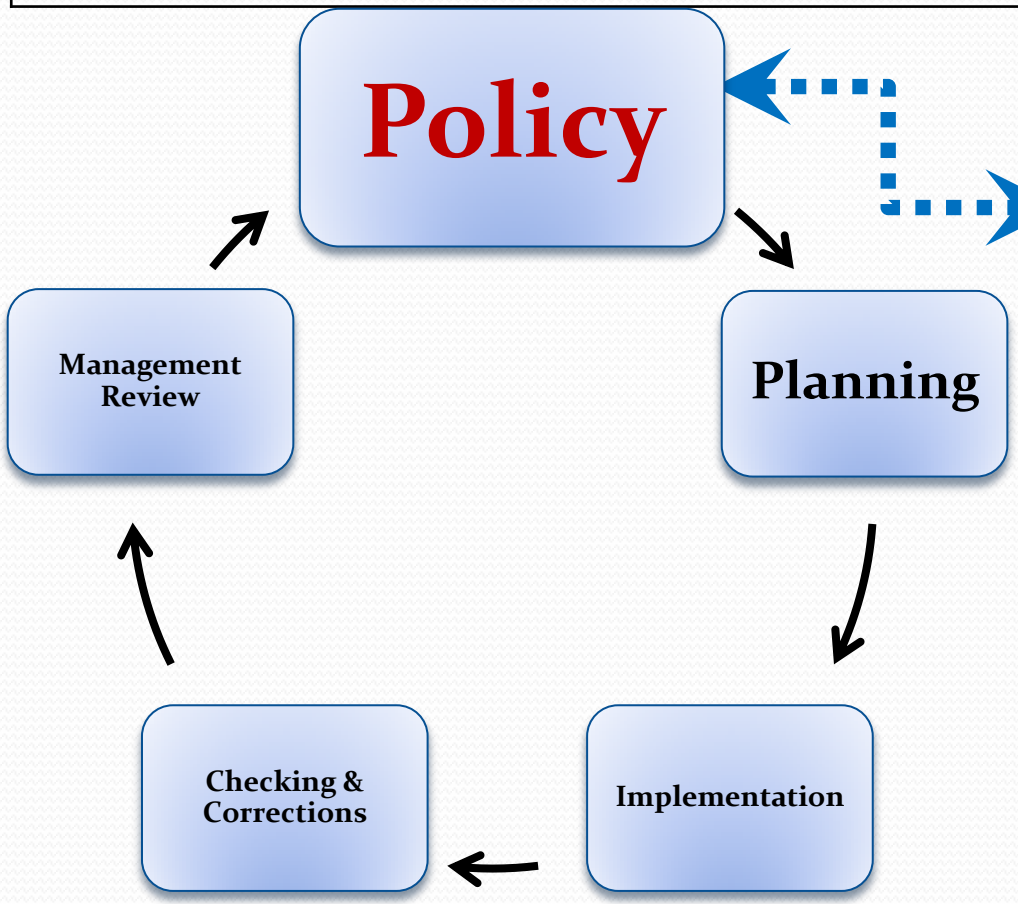
Enough D.I.K.C. at each system level?

Develop D.I.K.C. Metrics!



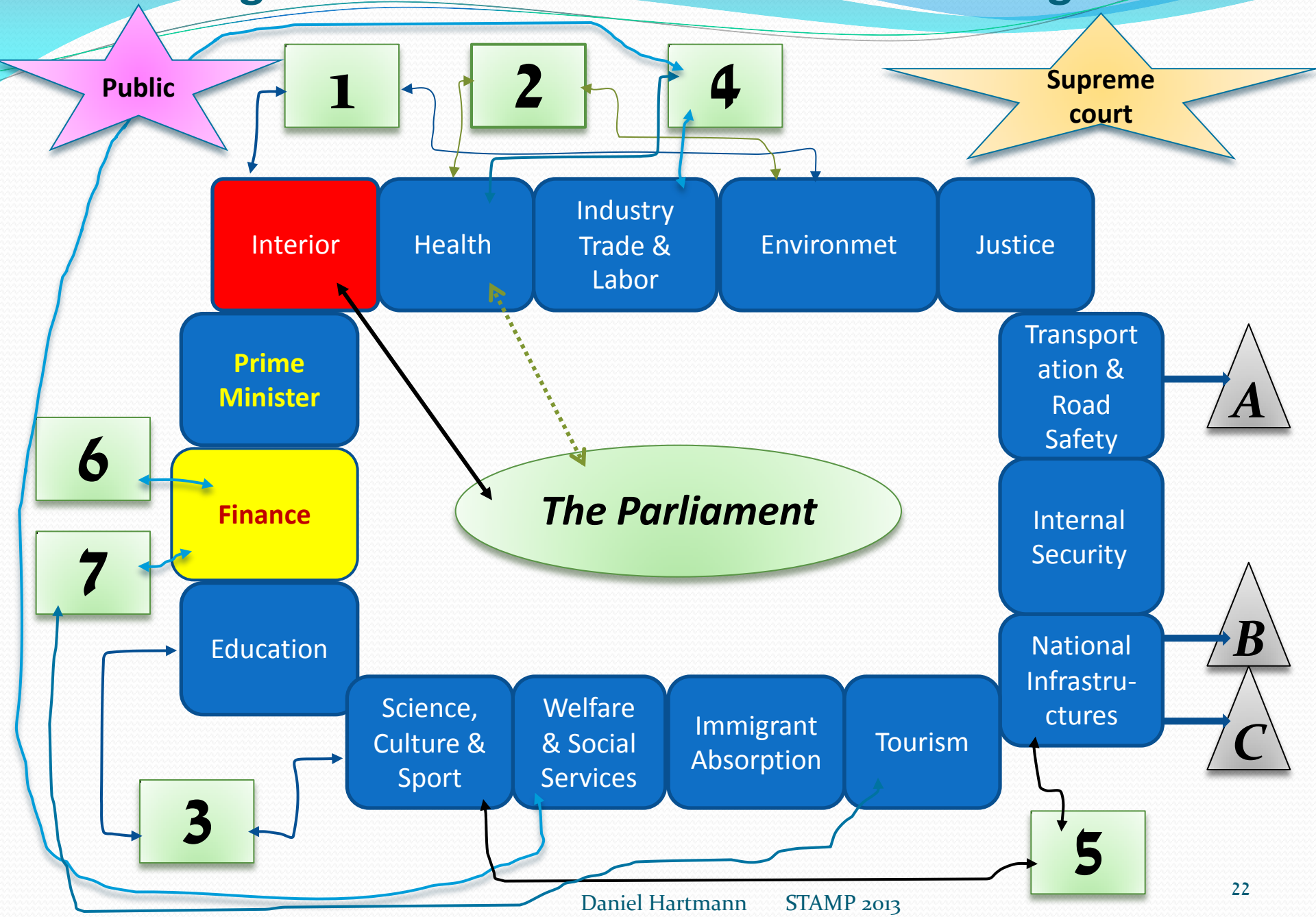
Generic model for safety management system

Level N+1	Goals, Policies, Constraints, Control Commands
Reference Channel ↓	Measuring Channel (Feedback) ↑
Level N Operational Experience	

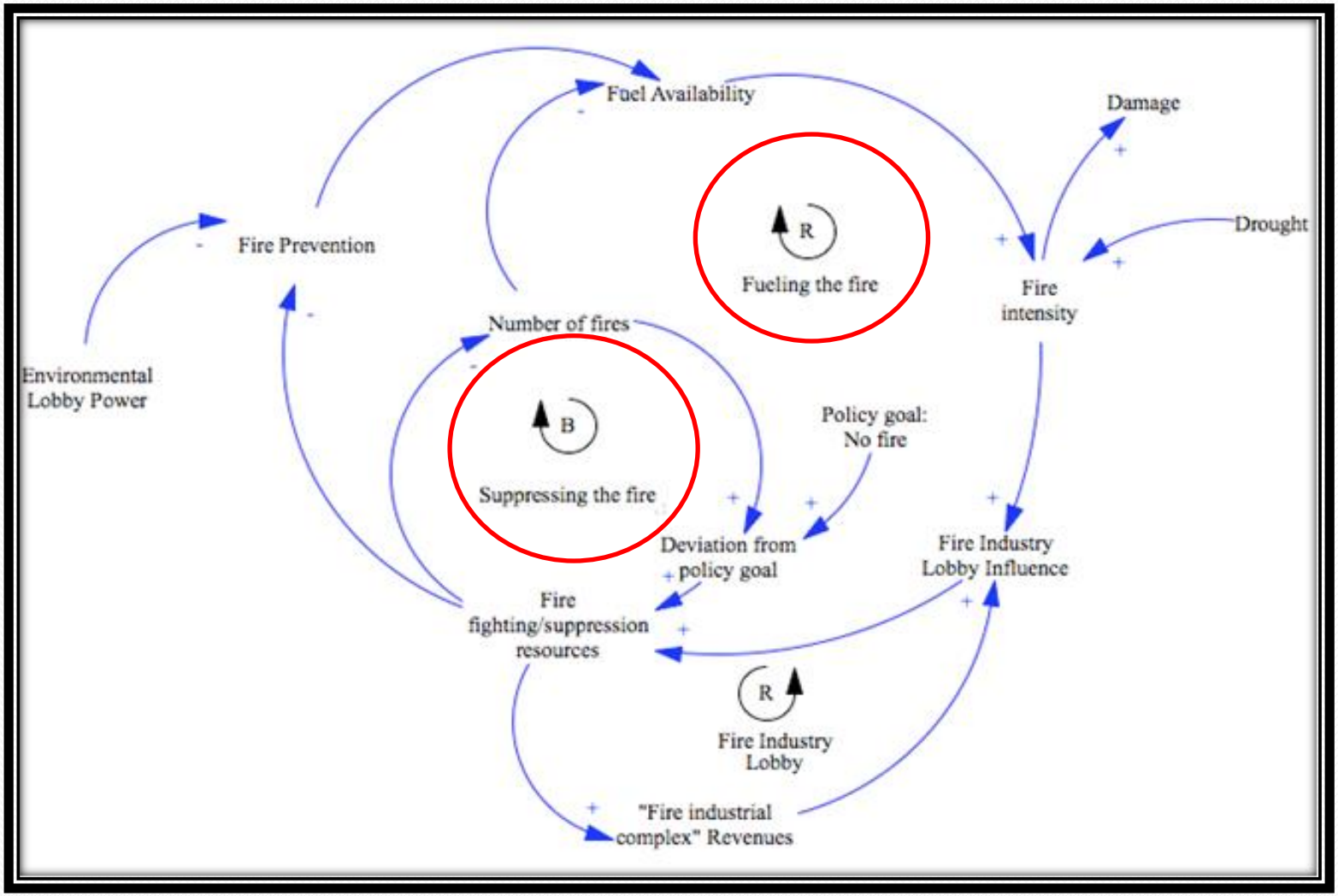


- Conflicting Policies
- Biased Policies
- Partial correct Policies
- Wrong Policies
- Unrealistic Policies
- Disastrous Policies
- Etc.

Drowning Prevention – Governmental Level Regulation



System Dynamics perspective on Forest Fire



Mount Carmel [Israel] forest fire (2010)

a very expensive lesson in risk management and safety

Reckoning without one's host

(die Rechnung ohne den Wirt machen)

- To act, plan, or conclude without adequate consideration of significant factors or circumstances;
- to fail to take into account the role of others, particularly those whose position would make their input determinative.
- This early meaning, dating from the 17th century, has been totally lost in the now figurative one indicating shortsightedness, improvidence, or lack of foresight.

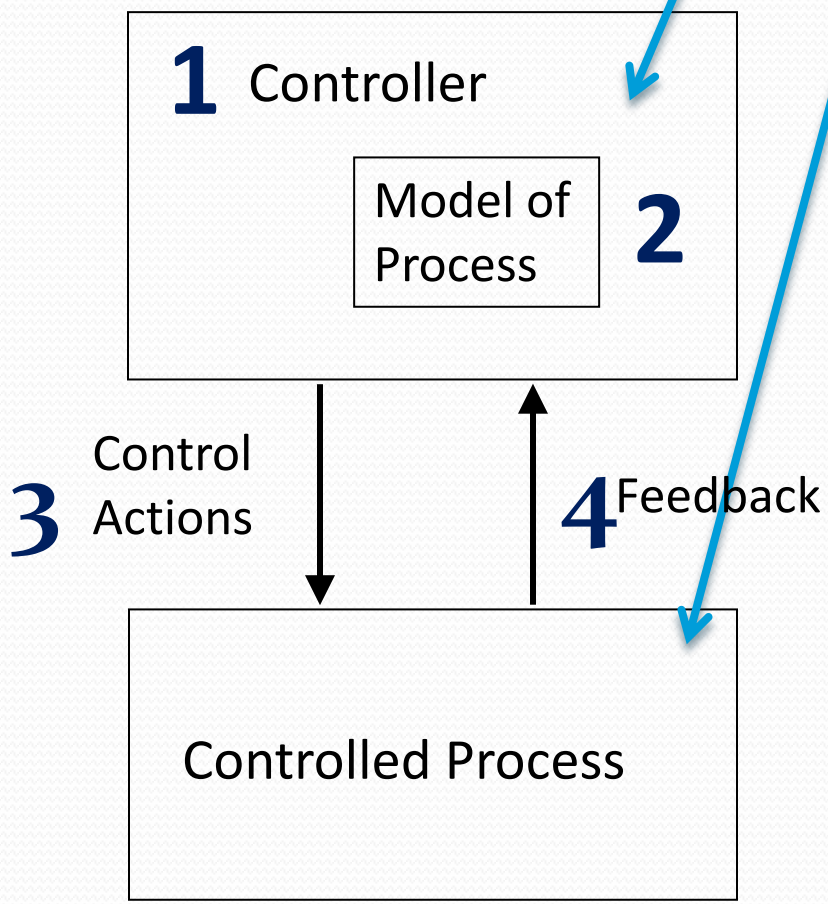
A wider look at STAMP

(System-Theoretic Accident Model and Processes)

- ➢ **Data – Information – Knowledge – Context [D.I.K.C.]**
- ✓ **System Theory**
- ✓ **Hierarchical Safety Control Structure**
- ✓ **Process Models**
- ✓ **Safety Constraints**

Control processes operate between levels of control

enough D.I.K.C. to create Models?



Process Models

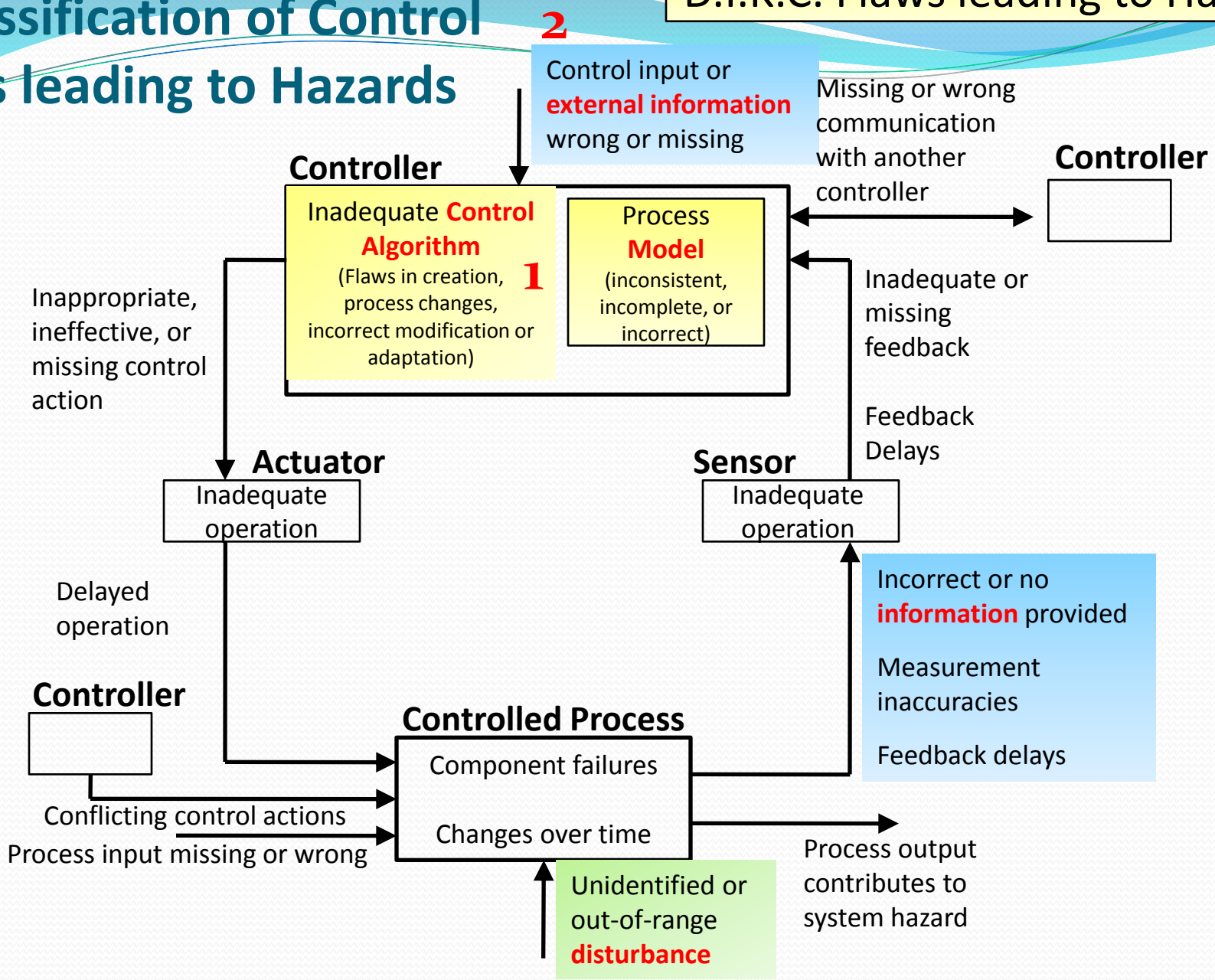
1. Goal Condition
2. Model Condition
3. Action Condition
4. Observability Condition

Accidents occur when model of process is inconsistent with real state of process and controller provides inadequate control actions

Feedback channels are critical
-- Design
-- Operation

A Classification of Control Flaws leading to Hazards

D.I.K.C. Flaws leading to Hazards



A wider look at STAMP

(System-Theoretic Accident Model and Processes)

- ➢ **Data – Information – Knowledge – Context [D.I.K.C.]**
- ✓ **System Theory**
- ✓ **Hierarchical Safety Control Structure**
- ✓ **Process Models**
- ✓ **Safety Constraints**

Safety Constraints
Should be based on D.I.K.C.: Data, Information, Knowledge & Context

- Based on D.I.K.C. Each component in the control structure has
  - Assigned responsibilities, authority, accountability
  - Controls that can be used to enforce safety constraints
- Based on D.I.K.C. Each component's behavior is influenced by
  - Context (milieu) in which operating
  - Level of Data, Information, Knowledge about current state of process

Relationship Between Safety and Process Models

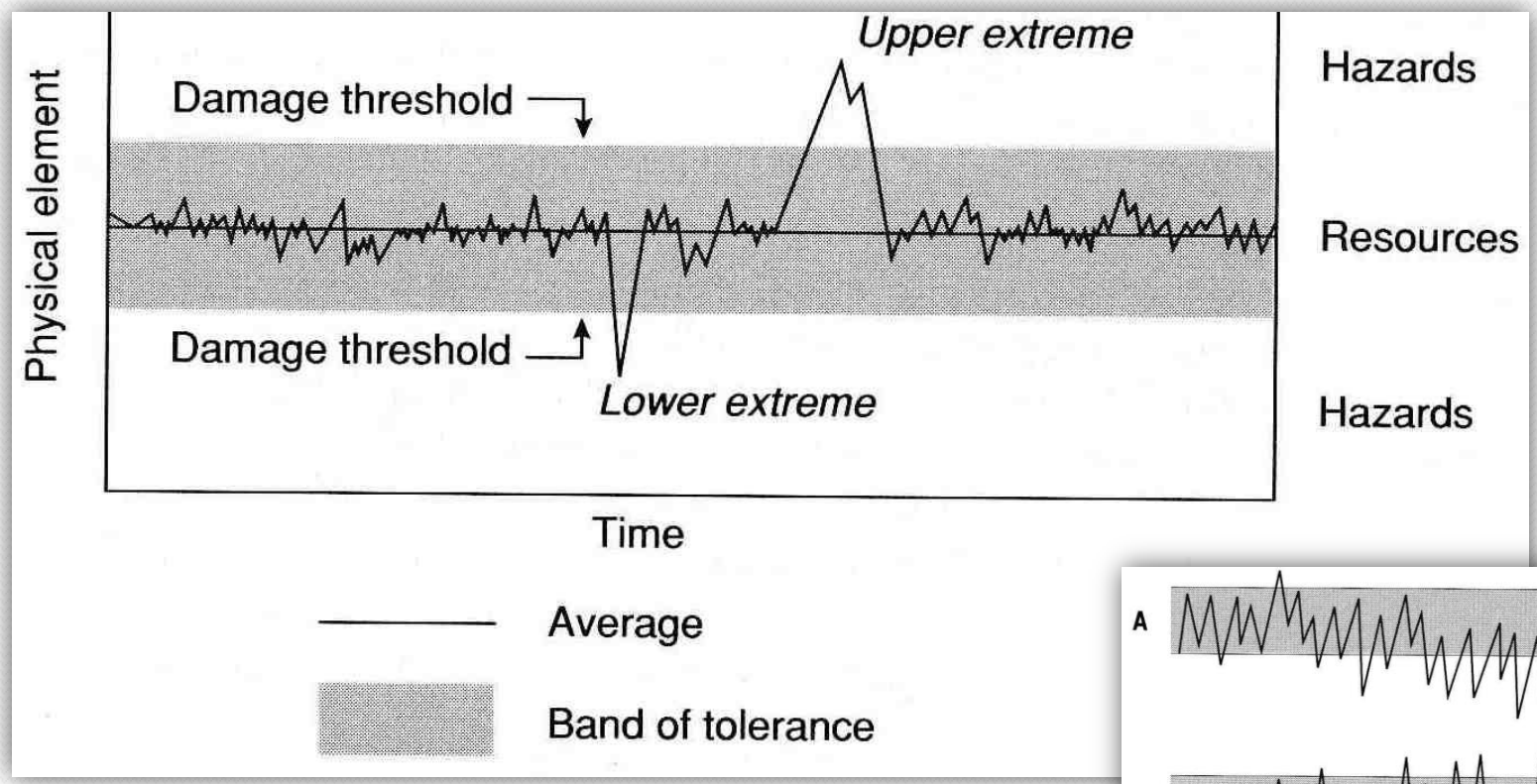
Depending on D.I.K.C. and level of D.I.K.C.

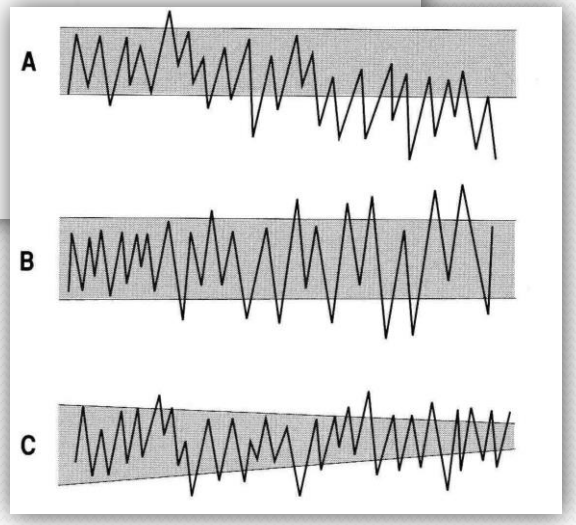
Accidents occur when models (because of D.I.K.C.) do not match process and:

- Required control commands are not given
- Incorrect (unsafe) ones are given
- Correct commands given at wrong time (too early, too late)
- Control stops too soon

Explains software errors, human errors, component interaction accidents, and errors due to level of DIK …

Human Sensitivity to Environmental Hazards





Levels of D.I.K.C., Level of Resolution of D.I.K.C. Levels of Processes & Hazards

Cosmological Climate?

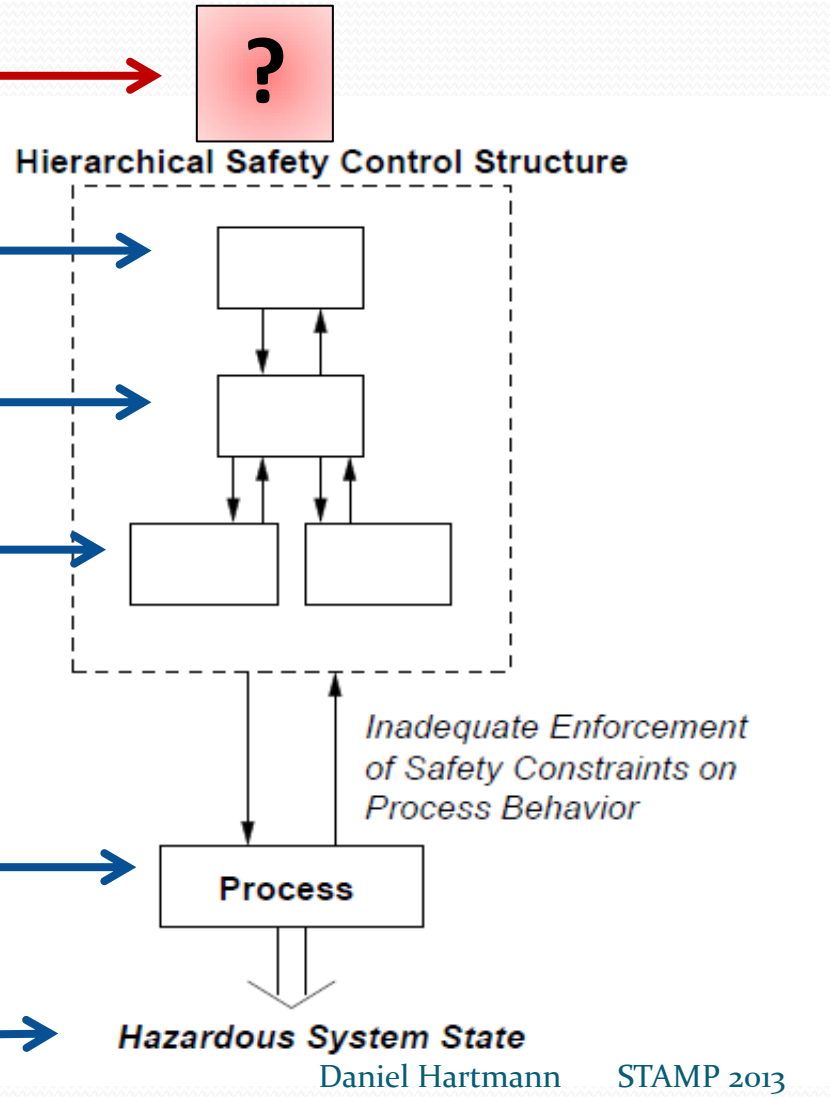
Geological Climate

Contemporary Climate

Weather

Climate Change

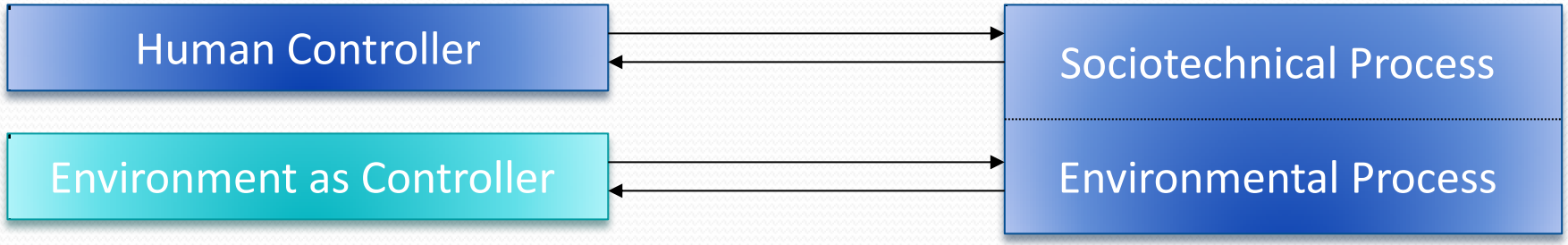
Hazards related to Climate Change



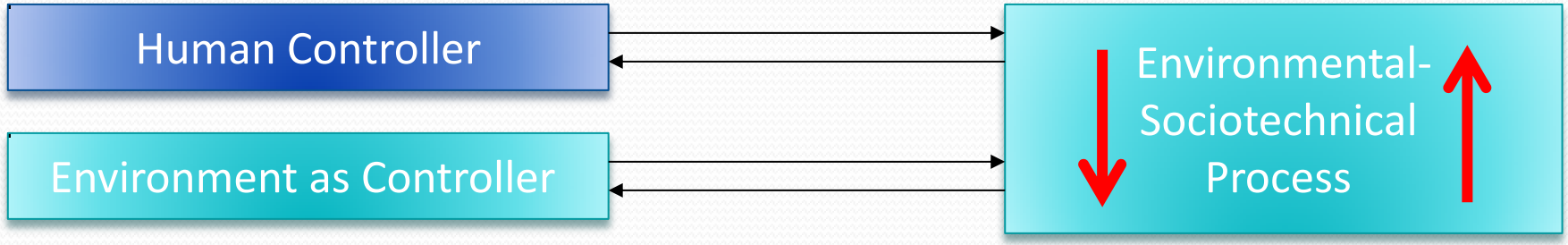
Another Source of Risk

- **Control actions inadequately "coordinated" among multiple controllers**

Boundary areas: Environmental conditions are "normal"



Overlap areas : Environmental conditions are "extreme"



Safety as a dynamic Control Problem

Sociotechnical system:

"enforce safety constraints on Sociotechnical system behavior"

Environmental-Sociotechnical system:

"enforce safety constraints on Sociotechnical system behavior and avoid confrontation with Environmental system behavior"

Dutch: Living / Building with Nature

THANKS

תודה רבה

HELP

Dr. Daniel Hartmann
Mail: danielh@bgu.ac.il